CHIPPING AWAY AT THE CONSTITUTION: THE INCREASING USE OF RFID CHIPS COULD LEAD TO AN EROSION OF PRIVACY RIGHTS

Reepal S. Dalal[*]

INTRODUCTION

Radio Frequency Identification, or RFID, is one of the latest technologies that will revolutionize the way we live. An RFID system involves the communication of digital data from an RFID chip or tag to a reader through radio waves.[1] It is similar to a Universal Product Code (UPC) system in which a barcode holds information that can be read by an infrared scan.[2] Unlike the barcode, RFID differs in its method of transmission and therefore does not

[*] J.D. Candidate, Boston University, 2006.

[1] RFID Basics – FAQs, http://www.zebra.com/id/zebra/na/en/index/rfid/faqs/rfid_basics.html (last visited Jan. 31, 2006).

[2] RFID & Bar Codes, http://www.zebra.com/id/zebra/na/en/index/rfid/faqs/rfid_bar_codes.html (last visited Jan. 31, 2006) (comparing the RFID and UPC systems).

require a direct line of sight.[3] Although the technology is still fairly new, its future uses could be extremely far-reaching. RFID systems are already being employed in various government and commercial contexts to track people and their movements,[4] farm animals,[5] and commercial products as they make their way from manufacturer to consumer.[6] As with many earlier tracking and surveillance technologies, the rise of such a vast information-gathering system implicates privacy concerns. An important question is where to strike the balance between the use of the technology to gather information for a more efficient society and the protection of individuals' Fourth Amendment rights against unreasonable search and seizure. As new technology is developed, the definition and scope of the Fourth Amendment must be revisited and interpreted in light of such advances.

This Note examines the use of RFID technology in various contexts and the potential privacy invasions that these uses create. Part I explores how RFID technology works, as well as its various applications in commercial and governmental contexts. Part II sets out the privacy concerns created by this technology. Part III analyzes whether the use of RFID systems constitutes a search under the Fourth Amendment and therefore presents a potential threat to individuals' Fourth Amendment rights. This analysis uses comparisons to previous courts' decisions about similar emerging technology to make predictions regarding the legal future of RFID. Part IV examines if and how intervening actions by a private party will affect the government's ability to obtain and use information compiled by private parties through the use of RFID technology. Finally, Part V discusses how some states have responded to emerging technologies similar to RFID by providing privacy protection above and beyond that provided by the Fourth Amendment, thus providing suggestions for how to deal with RFID.

---

[3] *See id.*

[4] Mark Baard, *RFID Keeps Track of Seniors*, WIRED, Mar. 19, 2004, http://www.wired.com/news/medtech/0,1286,62723,00.html (promoting the use of RFID to track "seniors' daily activities by recording which tagged items they have picked up" as well as tracking whether they have taken their necessary medications); How Does RFID Work in Schools?, http://www.rfidbuzz.com/news/2005/how_does_rfid_work_in_schools.html (last visited Jan. 31, 2006) (describing use of RFID to efficiently track absent and late students); Joanie Wexler, *Legoland Uses Both RFID, Wi-Fi to Find Lost Kids*, NETWORK WORLD, Apr. 26, 2004, http://www.networkworld.com/newsletters/wireless/2004/0426wireless1.html (explaining the benefits to parents of using RFID track their children in crowded places like amusement parks).

[5] RFID Microchips & GPS ID for all Farm Animals?, Oct. 17, 2005, http://arizona.indymedia.org/news/2005/10/31715.php (outlining a proposed regulation by the United States Department of Agriculture to use RFID microchips and Global Positioning System (GPS) identifiers to track farm animals across the country).

[6] *See Walmart RFID Pilot at Texas Distribution Centers*, RFIDA, http://www.rfida.com/data/walmartpilot.htm (last visited Jan. 31, 2006).

I. RFID: HOW DOES IT WORK AND WHERE IS IT USED?

A. *How the RFID System Works*

RFID is a method of identifying items using radio waves. There are two main components to an RFID system: a transponder, sometimes called a tag or a microchip, and a reader.[7] Generally, tags are attached to items and hold digital information about the item; the reader is used to extract the information held on the tag.[8]

The standardized coding system used to hold the information is called the Electronic Product Code, or EPC.[9] The EPC is conceptually similar to the UPC used in barcodes, but EPCs are more versatile than UPCs and can hold much more information.[10] While UPC barcodes can only store seven bits of information, EPC RFID tags can store up to 256 bits.[11] In fact, the EPC system has enough capacity "to provide unique identifiers for all items produced worldwide."[12] Information can be 'written onto' an EPC while it is affixed to an item, allowing the tag to continually update the item's information.[13] This means that as an item moves from one place to the next, the EPC is updated with information regarding its exact location.[14] Furthermore, the EPC system does not require line of sight in order to read information.[15] Therefore, a reader can pick up a signal emitted from an RFID

[7] Jeffrey K. Brecht, *Radio Frequency Identification (RFID) Technology*, http://foodsafety.ifas.ufl.edu/FSQA%20Update%202004/JKB%20RFID%20(5-04).pdf (last visited Jan. 31, 2006) (describing the basics of RFID technology, how it works, and common uses).

[8] *Id*. (illustrating how the tags store and convey information).

[9] What is EPC?, http://www.rfid.ie/whatisepc.html (last visited Jan. 31, 2006).

[10] *Id.*

[11] Jerry Brito, Note, *Relax, Don't Do It: Why RFID Privacy Concerns Are Exaggerated and Legislation Is Premature*, 2004 UCLA J.L. & TECH. 5, 12 (comparing the properties of the UPC and EPC technologies).

[12] RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, Nov. 20, 2003, http://www.privacyrights.org/ar/RFIDposition.htm.

[13] *See The History of RFID Technology*, RFID JOURNAL, http://www.rfidjournal.com/article/articleprint/1338/-1/129, (last visited Jan. 31, 2006) [hereinafter *History of RFID*] ("Data associated with the serial number on the tag would be stored in a database that would be accessible over the internet").

[14] *Id.*.

[15] Alex Goldman & Ken Crawford, *Five RFID Myths Exposed*, WI-FI PLANET, Jan. 6, 2004, http://www.wi-fiplanet.com/tutorials/article.php/3296031 ("With RFID, non line of sight (NLOS) interrogation is possible.").

tag without making a direct scan of the tag.[16] A variety of information can be transmitted by the tag.[17]

B. *Various Uses of RFID Technology*

1. Commercial Use

At the moment, commercial use of RFID technology to expedite supply chain response time is one of the most widespread uses of the technology. Advocates are hopeful that the new system will improve lower operating costs through "labor reduction and efficient business process."[18] Wal-Mart was the first to implement the technology, and other retailers are beginning to invest in the system by asking their suppliers to place RFID tags on all pallets and cases that are delivered.[19] Gillette was one of eight suppliers willing to participate in the pilot program with Wal-Mart, and because Gillette believes that the benefits will be greater the earlier in the process it can tag goods, the company has also "launched a pilot to tag at the source at its packaging facility."[20] Eventually, retailers hope to place scanners on shelves to give real time information about the quantity of an item, which will in turn speed up restocking processes.[21]

Another contemplated use for RFID tags is to track luggage on airlines.[22] Use of RFID in this context could reduce the occurrences of late, lost, and misrouted airline luggage.[23] The RFID system would allow the airline to "automatically tag, sort and route bags, far faster and more reliably" than the current bar code system.[24] The tags can also be updated with any new or changing information regarding revised flights or rerouting information.[25]

---

[16] *See id.* ("With circular polarized antennas, the beam does not need to be oriented manually, as it may have to be with a linear bar code.").

[17] *Definition of RFID*, WORDIQ, http://www.wordiq.com/definition/Rfid (last visited Jan. 31, 2006) (describing the many current uses of RFID technology, including but not limited to: identification or location information, and specific information about the product tagged, such as price, color, and date of purchase).

[18] *Walmart RFID Pilot at Texas Distribution Centers*, *supra* note 6.

[19] *See* Carol Sliwa, *Gillette Shaves Costs with RFID*, TECHWORLD.COM, Jan. 5, 2005, http://www.techworld.com/mobility/features/index.cfm?FeatureID=1090 (describing the increased use of RFID technology in the supply chain process).

[20] *Id*.

[21] Brecht, *supra* note 7 (describing potential uses of RFID technology in various industries).

[22] *Id.*

[23] Press Release, Texas Instruments, Texas Instruments Radio Frequency ID (RFID) System, Tag-it™, Continues Trials for British Airways Baggage Handling (Jan. 25, 1999), *available at* http://www.ti.com/rfid/docs/news/news_releases/90s/rel01-25-99.shtml.

[24] *Id.*

[25] *Id.*

In a more extreme example, RFID tags are being used as human tracking devices.[26] "A children's theme park in Denmark is using a combination of wireless technologies to track . . . kids gone astray."[27] The service offered at the park allows parents to rent a wristband for their children that contains a Wi-Fi-enhanced RFID tag.[28] Using RFID in this manner illustrates the "synergies emerging between wireless technologies."[29] The system works by attaching the wristband to the child's arm; then, at any time, the parent can send a short message service (SMS) query to the system and the parent will receive a return message containing their child's location.[30] Although this seems like a pragmatic system in light of recent heightened fears of child abduction, the potential for human tracking taken beyond the child context has raised many concerns with privacy advocates.[31]

2. Government Use

While increased consumer use of RFID is more likely in the near future, the government has also expanded its use of the technology. One of the first government uses of this type of technology was to identify approaching aircraft.[32] Additionally, the U.S Energy Department is using RFID to develop a method to track nuclear materials.[33]

One of the potential government uses of RFID technology involves placing the information chips inside passports.[34] The U.S. government plans to issue diplomats and State Department employees new passports containing RFID chips, and allow other citizens to receive the RFID version as they apply for new or renewed passports.[35] The government is hoping that all new passports, beginning in 2006, will contain biometric data.[36] The information transmitted

[26] Wexler, *supra* note 4.

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] *See* Waseem Karim, Note, *The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring*, 14 WASH. U.J.L. & POL'Y 485, 492, 494-96 (2004).

[32] *History of RFID, supra* note 13 (relating how during World War II, German pilots would roll their planes as they approached the airfield, alerting the radar crew on the ground that these were German planes and not Allied aircraft).

[33] *Id.*

[34] *See* Ryan Singel, *American Passports to Get Chipped*, WIRED NEWS, Oct. 21, 2004, http://web.archive.org/web/20050401094123/http://www.wired.com/news/privacy/0,1848,65412,00.html.

[35] *Id.*

[36] Tresa Baldas, *Little Chip Evokes Big Brother*, NAT'L L.J., Oct. 4, 2004 ("Biometrics is the use of biological properties, such as fingerprints or retina scans . . . to identify subjects.").

from the RFID chip to the reader would likely include the passport holder's name, address, date and place of birth, as well as a digital photograph.[37] In addition to this personal information, the tag would also transmit a digital signature verifying that the chip was created by the government.[38] The goal would be to make forgeries of U.S. passports more difficult.[39]

Another potential government use of the technology involves chips placed in driver's licenses. For reasons similar to those advanced for placing RFID tags in passports, some states have considered placing RFID tags in drivers' licenses to thwart counterfeits and forgeries.[40] Virginia was one of the first states to consider the new licenses as a response to the September 2001 terrorist attacks.[41] "'Nine of the 19 9/11 terrorists obtained their licenses illegally in Virginia, and that was quite an embarrassment,' said Virginia General Assembly delegate Kathy Byron, chairwoman of a subcommittee looking into the use of so-called smart driver's licenses which may contain RFID technology."[42] The RFID tags would make the licenses a "contact-less" technology; allow for more efficient identification verification; and help lines at security checkpoints move more quickly.[43] If federal legislators mandate RFID chips in driver's licenses, licenses could then become national identification cards that could be read remotely throughout the country.[44]

In the past few years, several states have expedited the collection of tolls on highways by instituting the use of "E-Z Pass" or "Fast Pass" systems which allow drivers to pay tolls without stopping their vehicles.[45] The system involves individuals purchasing transponders for their cars. The drivers purchase a prepaid balance, which is stored on the transponder.[46] As the car passes through the toll booth the appropriate amount of toll is deducted from the prepaid balance by the use of an RFID reader attached to the toll booth.[47]

---

[37] Singel, *supra* note 34.

[38] *Id.*

[39] *See id.*

[40] Mark Baard, *RFID Driver's Licenses Debated*, WIRED NEWS, Oct. 6, 2004, http://www.wired.com/news/privacy/0,1848,65243,00.html [hereinafter Baard, *Driver's Licenses*] (explaining that use of the "tags may prevent identity fraud and help thwart terrorists using falsified documents to move about the country").

[41] *Id.* ("Virginia is among the first states to explore the idea of creating a smart driver's license, which may eventually use any combination of RFID tags and biometric data, such as fingerprints or retinal scans.").

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] Jimmy Atkinson & Andy Hagans, *RFID Found at Highway Toll Booths*, RFID GAZETTE, Mar. 24, 2005, http://www.rfidgazette.org/2005/03/rfid_found_at_h.html (applauding the new technology's ability to "save[] lots of time and increase[] traffic flow").

[46] Kevin Bonsor, *How E-ZPass Works*, HOWSTUFFWORKS, http://auto.howstuffworks.com/e-zpass2.htm (last visited Jan. 30, 2006).

[47] *See id.*

As RFID does not require line of sight, the car does not have to come to a complete stop for the reader on the toll booth and the transponder in the car to communicate.[48] This innovation has reduced commute times for travelers and reduced the city's need for toll booth collectors.[49]

II. PRIVACY CONCERNS EXPLAINED

A. *Commercial Use Privacy Concerns*

One of the most frequently voiced concerns about RFID technology involves its use in the commercial context.[50] This is likely because the proposal to eventually place RFID tags in all consumer products would probably constitute its most widespread usage and therefore affect the largest number of people. RFID opponents argue that extensive commercial use could "create a total surveillance world" by using RFID tags on items purchased by consumers to track citizens anywhere in the country.[51] If RFID tags are attached to consumer goods such as shoes, then wearers could be tracked everywhere they go.[52] Another concern is that if all the items in citizens' homes have RFID tags, then a person passing by, whether a potential criminal or a police officer, could point an RFID reader into the home and learn the contents of the home.[53]

This concern would be alleviated somewhat by imposing "kill" regulations which require the retailer to deactivate (or "kill") the "live" RFID tags before they leave the store.[54] There is still concern, however, that not all tags will actually be killed as they depart stores and thus the potential for tracking

---

[48] *See* Atkinson & Hagans, *supra* note 45 (explaining that this feature of the new technology helps to increase traffic flow).

[49] *Id.*

[50] *See The ROI of Privacy Invasion*, ASSOCIATION FOR AUTOMATIC IDENTIFICATION AND MOBILITY (AIM) GLOBAL, Jan. 2004, http://www.aimglobal.org/technologies/rfid/resources/articles/jan04/0401-roispy.htm (surveying many of the more alarmist privacy concerns voiced regarding the use of RFID tags).

[51] *Id.*

[52] *Id.* ("Readers in the floors of malls, [opponents of the technology] suggest, could read the EPC tag in your shoes (which might have been put there without your knowledge). Given this scenario, you could be tracked wherever you go.").

[53] *Id.*; *see* Mark Baard, *Watchdogs Push for RFID Laws*, WIRED NEWS, Apr. 5, 2004, http://www.wired.com/news/politics/privacy/0,62922-0.html?tw=wn_technology_security_3 [hereinafter Baard, *Watchdogs*] ("RFID will make it easy for companies and government investigators to establish the whereabouts of citizens, by reading the active tags on their clothing and other items in private and public places.").

[54] *See Privacy Gets on the Agenda*, RFID JOURNAL, Nov. 20, 2005, http://www.rfidjournal.com/article/articleview/1556/1/159.

people's movements and belongings would still exist.[55] More alarming is the opposition to implementing the "kill tag" rule.[56] "[Proctor & Gamble] and other companies . . . suggested they want to keep RFID tags active after checkout, rather than disabling them with so-called 'kill machines.'"[57] The companies would benefit by being able to profile their shoppers, though the companies argue that consumers would also benefit by being able to return goods without a receipt.[58]

The prospect of private companies creating extensive information databases on individuals through the commercial use of RFID technology is alarming. In addition to creating profiles on individuals, there is a growing concern that private companies might share the information they have gathered with the government, which could lead to intrusive government surveillance and profiling.[59] The Department of Homeland Security has been working with companies such as Wal-Mart and Procter & Gamble to develop the use of RFID systems in the Department's operations.[60] "Homeland Security may find the combination of live tags and customer profiles hard to resist when investigating suspected terrorists, or as a means to monitor entire groups of people . . . ."[61] Although the Privacy Act of 1974 does not allow the government to maintain profiles on individuals who are not targets of investigations, the government is not prohibited from purchasing such information from private organizations.[62] This concern is heightened by reports that "the Justice Department has an eight million dollar contract with Choicepoint, a data collection company, for access to their databases of personal information."[63] The ability to access the information gathered by

[55] *See* Baard, *Watchdogs*, s*upra* note 53; *see also Position Statement on the Use of RFID on Consumer Products*, ELECTRONIC FRONTIER FOUNDATION, Nov. 14, 2003, http://www.eff.org/Privacy/Surveillance/RFID/rfid_position_statement.php.

[56] *See* Baard, *Watchdogs*, s*upra* note 53.

[57] *Id.*

[58] *Id.*

[59] *See id.* ("[C]ompanies could use RFID tags to profile their own customers and share their information with the government . . . .").

[60] *Id.*

[61] *Id.*

[62] Karim, *supra* note 31, at 501-02 (discussing the government's "capability to consolidate . . . information and to create all-inclusive profiles on individuals"); *see generally* Jay Stanley & Barry Steinhardt, AMERICAN CIVIL LIBERTIES UNION, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, (ACLU/Technology and Liberty Program), Jan. 2003, *available at* http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf (describing the overall impact of surveillance devices on privacy in the United States).

[63] Karim, *supra* note 31. For documents detailing the contracts between United States government agencies and ChoicePoint, see *ChoicePoint, Autopoint XP: International Searches*, ELECTRONIC PRIVACY INFORMATION CENTER, Sept. 12, 2001, http://www.epic.org/privacy/publicrecords/inschoicepoint.pdf; *ChoicePoint*, ELECTRONIC

private companies and organizations demonstrates the potential for Fourth Amendment violations by the government arising from commercial uses of RFID technology.

B. *Government Use Privacy Concerns*

The most significant concern surrounding government use of RFID is the limitless surveillance potential. Government use of various technologies for surveillance purposes has always been a highly litigated issue, and the Supreme Court has been frequently called upon to strike a balance between proper and improper uses of technology.[64] Surveillance technology is ever-advancing and the courts must continually interpret and draw lines between permissible uses and those which violate individuals' Fourth Amendment rights. The potential government applications of RFID technology examined in the following sections justify the growing concern about widespread government surveillance.

1. Passport / Driver's License Concerns

Although equipping passports and driver's licenses with RFID tags presents many advantages for security, there is also a downside. Passports and driver's licenses contain highly sensitive personal information about citizens' whereabouts and identity. The recent attention given to identity theft has shed light on the immense harm that could result if personal information falls in the wrong hands.[65] However, privacy advocates are more concerned that government officials will be able to lawfully access personal information from citizens' passports and driver's licenses without citizens' knowledge or consent.[66] Because the information from the chips can be read remotely,[67] "[p]utting the chips in passports would enable the government to read personal information from more than 50 feet away."[68] Eventually "[i]nformation from card readers could also be coupled with global positioning system data and relayed to satellites, helping the government form a comprehensive picture of the comings and goings of its citizens."[69]

PRIVACY INFORMATION CENTER, July 6, 2001, http://www.epic.org/privacy/publicrecords/citizenprices.pdf.

[64] *See infra* Parts III-V (analyzing the Fourth Amendment implications of the use of RFID technology).

[65] *See* Jon Cohen, *Poll: Identity Theft Concerns Rise*, ABC NEWS, Mar. 17, 2005, http://abcnews.go.com/Business/PollVault/story?id=590413&page=1.

[66] *See* Baldas, *supra* note 36.

[67] Baard, *Driver's Licenses*, *supra* note 40.

[68] John Carey, *Big Brother's Passport to Pry*, BUSINESSWEEK ONLINE, Nov. 5, 2004, http://www.businessweek.com/bwdaily/dnflash/nov2004/nf2004115_1663_db016.htm.

[69] Baard, *Driver's Licenses*, *supra* note 40.

2. Toll Collection Concerns

While the use of RFID in toll collection booths has produced immediate and noticeable improvements in traffic to many commuters, this too has a downside. This use allows information to be gathered regarding the travel of citizens' cars on highways. The surveillance potential is immense. "Investigators in criminal investigations already regularly subpoena E-Z Pass automatic toll records, which come from RFID readers, to figure out where an individual's car was at a particular time."[70]

The possibility of the government profiling individuals is also a concern raised by government use of RFID. Much like the concern that the government will purchase information from private companies to create profiles, the government could also use the information it obtains through its own uses to create such profiles.[71] The government's own implementation of RFID systems simply eliminates the need to contract with a private company; instead government officials have direct access to information regarding individuals' whereabouts and lifestyles. Profiling can be seen and is analyzed as an enhanced form of surveillance.[72]

The potential for abuse created by these surveillance capabilities by the government has fueled a "big brother" scare which seems to have been reignited by the recently passed USA PATRIOT Act ("Act").[73] The Act broadens federal law enforcement's authority by expanding terrorism laws to include "domestic terrorism."[74] The Act also increases, among other things, law enforcement's power to conduct searches, as well as its ability to use phone and internet surveillance techniques[75] This legislation has prompted significant opposition in light of its threats to citizens' civil liberties.[76] Given this expanded government authority, concerns are brewing regarding the

[70] Baard, *Watchdogs*, *supra* note 53.

[71] *See* Karim, *supra* note 31, at 501-02 ("Where corporations have the potential to collect data about individuals for their use, the government has the capability to consolidate the information and to create all-inclusive profiles on individuals.").

[72] *See Radio Frequency Identification (RFID) Systems*, ELECTRONIC PRIVACY INFORMATION CENTER, http://www.epic.org/privacy/rfid/ (last visited Feb. 1, 2006) (pointing out critics' fears that RFID readers could be used by the government to gather information and maintain surveillance of citizens).

[73] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (to be codified at 18 U.S.C. 2517(6)); *see also* Baldas, *supra* note 36.

[74] United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, Pub. L. 107-56, § 802, 115 Stat. 272 (2001).

[75] *Id.* §§ 201 – 203, 213.

[76] *See, e.g.*, *Radio Frequency Identification (RFID) Systems*, *supra* note 72.

potential for government use of RFID technology to infringe on citizens' Fourth Amendment rights.[77]

III. FOURTH AMENDMENT ANALYSIS

Although the contemplated future uses of RFID technology and their Fourth Amendment implications have not yet been analyzed by the courts, the constitutional limits of government surveillance have been highly contested.[78] The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.[79]

The purpose of the Fourth Amendment is to protect individuals within the United States from government intrusion by means of unreasonable search and seizure.[80] Interpretation of the scope of this Amendment has evolved over the years. The principle cases analyzing and establishing the parameters of the Fourth Amendment provide the starting point for determining how courts will balance concern over individual privacy rights with the emerging (and frequently beneficial) uses of radio frequency technology. Two key questions must be addressed when applying the Fourth Amendment's protections to RFID technology: (1) whether use of the technology by the government would be considered a "search" within the scope of the Fourth Amendment,[81] and if so, (2) whether the search is unreasonable under that Amendment.[82]

A. *What Is a "Search"?*

Over the years the Supreme Court has modified and expanded its definition of a search within the context of the Fourth Amendment. In 1928, the Court decided *Olmstead v. United States*, which involved the government's use of wiretapping to gain evidence of the defendant's role in a conspiracy to violate

---

[77] *See* Doug Campbell, *RFID Policy May Not Wait*, RFID JOURNAL, Mar. 28, 2005, http://www.rfidjournal.com/article/articleview/1461/1/128/

[78] *See, e.g.*, Kyllo v. United States, 533 U.S. 29 (2001); United States v. Knotts, 460 U.S. 276 (1983); United States v. McIver, 186 F.3d 1119, (1999).

[79] U.S. CONST. amend. IV.

[80] *See* Jennifer C. Evans, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001*, 33 LOY. U. CHI. L.J. 933, 936-37 (2002) (discussing the interference on civil liberties by legislation passed under the semblance of national security).

[81] *See* Katz v. United States, 389 U.S. 347, 351-52 (1967); *see also infra* Part III.A (discussing the definition of a search in the context of the Fourth Amendment).

[82] *See id.* at 361; *see also infra* Part III.B (analyzing the formulation and application of a two-part test to determine whether a search conducted by the government would qualify as an unreasonable search and seizure under the Fourth Amendment).

the National Prohibition Act.[83] The primary issue at hand was whether this case involved a search within the meaning of the Fourth Amendment.[84] In the majority opinion, Chief Justice Taft examined the Fourth Amendment's application in several previous cases.[85] Those cases did not involve the use of wiretapping or eavesdropping on phone calls, or the use of any other type of surveillance technology.[86] The Court thus had to confront the distinction between physical and technological intrusions in deciding *Olmstead*.[87]

The Court recognized that among its previous decisions, *Gouled v. United States* employed the most liberal construction of the Fourth Amendment.[88] That case involved a private in the U.S. Army who gained access to the defendant's office (by pretending to make a friendly visit) and then left with several documents.[89] In finding the acts of the Army private unconstitutional, the Court stated that "[a] stealthy entrance . . . became the equivalent to an entry by force."[90] At the time that *Olmstead* was decided, the Court was not willing to extend the meaning of a Fourth Amendment search beyond the parameters enunciated in *Gouled*.[91] In ruling that the government had legally obtained the evidence, the Court stated "[t]he language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are

[83] 277 U.S. 438, 455 (1928) (announcing that the sole issue in the case is "whether the use of evidence of private telephone conversations . . . intercepted by means of wiretapping, amounted to a violation of the Fourth and Fifth Amendments").

[84] *Id.*

[85] *Id.* at 458.

[86] *See id.* at 458-62. Chief Justice Taft examines the application of several previous cases involving the Fourth Amendment. Included in his analysis is the case of *Weeks v. United States*, 232 U.S. 383 (1914), in which the defendant was arrested by a police officer at his home and, while detained, law enforcement officials searched and took possession of various documents and articles without a search warrant. This was ruled to be an unconstitutional search under the Fourth Amendment. *Olmstead*, 277 U.S. at 460. Similarly, in the case of *Silverthorne Lumber Co. v. United States*, a government official's search of the defendants' office and seizure of all the books, papers and documents found there while the defendants were detained was found to be unconstitutional. 251 U.S. 385 (1920).

[87] *See id.* at 466.

[88] *See id.* at 463 ("*Gouled v. United States* carried the inhibition against unreasonable searches and seizures to the extreme limit."). The court went on to state that the authority of the Fourth Amendment should not be extended beyond the specific facts of the *Gouled* case. *Id.*

[89] *Id.* at 462.

[90] *Id.* at 463-64.

[91] *See id.* ("[Gouled's] authority is not to be enlarged by implication and must be confined to the precise state of facts disclosed by the record.").

stretched."[92] Accordingly, the Court concluded that "wire tapping . . . did not amount to a search or seizure within the meaning of the Fourth Amendment."[93]

The scope of "search and seizure" established by *Olmstead* endured for almost forty years, until the Court overturned *Olmstead* when it decided *Katz v. United States*.[94] In *Katz*, the Court stated that "the underpinnings of *Olmstead* . . . have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling."[95] One of those subsequent decisions was *Silverman v. United States*, which expanded the Fourth Amendment to searches that do not involve an actual physical intrusion.[96] The *Silverman* Court stated that the "Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any 'technical trespass under . . . local property law.'"[97] In *Warden v. Hayden*, a subsequent decision involving the scope of Fourth Amendment rights, the Court stated that "[t]he premise that property interests control the right of the Government to search and seize has been discredited."[98] That decision, along with *Silverman*, expanded the scope of the Fourth Amendment and overturned the rationale in *Olmstead* by recognizing the need for reexamination of constitutional principles "in the light of . . . developments in the science of electronics."[99] Together, these cases have created the overriding principle that the "Fourth Amendment protects people, not places,"[100] and have expanded the realm of the Fourth Amendment to protect people from electronic invasions, not just physical invasions of privacy.

If *Olmstead* still defined the current state of the Fourth Amendment's expanse, then the use of RFID technology would undoubtedly not fall within the Amendment's protections. Because RFID technology does not involve even a direct line of sight from reader to transponder to gather information,

[92] *Id.* at 465.

[93] *Id.* at 466.

[94] 389 U.S. 347 (1967).

[95] *Id.* at 353.

[96] 365 U.S. 505, 511 (1961); *see Katz*, 389 U.S. at 353.

[97] Silverman, 365 U.S. at 511. *Silverman* involved police officers who used a "spike mike" to eavesdrop on conversations in a building where they suspected illegal gambling was taking place. *Id.* at 505. Evidence of those conversations was ruled inadmissible because it was obtained by means of an unauthorized penetration into the premises of the defendant and therefore in violation of the defendant's Fourth Amendment rights. *Id.* at 506.

[98] 387 U.S. 294, 304 (1976) (discussing the purpose of the Fourth Amendment and further stating that the "principal object of the Fourth Amendment is the protection of privacy rather than property").

[99] *Silverman*, 365 U.S. at 508; *see also Warden*, 387 U.S. at 304 (explaining that the Court has "increasingly discarded fictional and procedural barriers rested on property concepts").

[100] *Katz*, 389 U.S. at 351.

much less a physical entry, the *Olmstead* requirement of physical intrusion would not be met and analysis under the Fourth Amendment would cease at this point.[101] But in rejecting *Olmstead*, the *Katz* Court's overriding principle was that a physical intrusion should not be necessary in order to find a "search" under the Fourth Amendment.[102] Additionally, by protecting people, rather than places, the case established that regardless of physical intrusion into a place, a search performed by any method – even in a public place – could constitute a search under the Fourth Amendment.[103] A search using RFID technology would likely be performed without any physical intrusion. Under the current state of the law, because a physical intrusion is not necessary to bring a search within the scope of the Fourth Amendment, the use of RFID technology would likely be a "search" subject to Fourth Amendment scrutiny.[104]

B. *Defining the Unreasonable Search: The Two-Part Test*

The *Katz* case declared a two-part test to determine when a search amounts to a constitutional violation.[105] This test governs whether a person invoking the Fourth Amendment's protection "can claim [that] a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy'" was infringed by the government.[106] In *Katz*, Justice Harlan formulated the test as follows: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[107] Therefore, although a person's home is considered his ultimate sanctuary where he should be free from government intrusion,[108] "objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them [private] has been exhibited."[109] This reasoning led to the Court's decision that

[101] *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

[102] *See Katz*, 389 U.S. at 351-52 (observing that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

[103] *Id.*

[104] *See infra* Part III.C.

[105] *Id.* at 361 (Harlan, J., concurring).

[106] United States v. Knotts, 460 U.S. 276, 280 (1983) (quoting Smith v. Maryland, 442 U.S. 735, 740-41 (1979)).

[107] *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Justice Harlan wrote his concurring opinion in order to express his differing view regarding the possibility that interception of a conversation in a public telephone may in some circumstances fall within an exception to the general rule that warrants are required. *See id.* at 360-62.

[108] *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961))).

[109] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

eavesdropping on a private conversation occurring within a public telephone booth was an unreasonable search within the meaning of the Fourth Amendment.[110] Although the telephone booth was in a public place, the fact that a person who occupies a telephone booth shuts the door behind him evidences his expectation that his conversation is private and free from government intrusion.[111] The principle of protecting people instead of places led the Supreme Court to hold in *California v. Ciraolo* that an unconstitutional search under the Fourth Amendment "does *not* occur – even when the explicitly protected location of a *house* is concerned – unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society [is] willing to recognize that expectation as reasonable.'"[112]

C. *Applying the Two-Part Test to Surveillance Technology*

The *Katz* test has been applied in numerous situations. A look at a few cases regarding various surveillance situations clarifies when the use of technology and surveillance equipment falls within the scope of an unreasonable search under the Fourth Amendment. *United States v. Knotts* involved governmental surveillance by means of a beeper that followed an automobile's movement on public streets and highways.[113] Aided by the beeper, the police were able to follow the automobile and were led to a cabin belonging to the defendants.[114] Upon locating the cabin, the police officers then proceeded to monitor the cabin for several days using video surveillance.[115] The information acquired through the surveillance of the cabin was subsequently used to obtain a search warrant, which led to the arrest and eventual conviction of the defendants for conspiracy to manufacture controlled substances.[116] In upholding the conviction, the *Knotts* Court held that there is a

[110] *See id.* at 352 (rejecting the government's contention that by using a public phone booth in which he was visible he essentially waived his right to Fourth Amendment protection).

[111] *Id.* ("One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

[112] 476 U.S. 207, 211 (1986).

[113] 460 U.S. 276, 277-80 (1983).

[114] *Id.* at 278-79.

[115] *Id*. at 279. In an attempt to catch an individual suspected of manufacturing illegal drugs, Minnesota law enforcement officers arranged with a seller of chloroform, which was used in the manufacture of the drugs, to place a beeper with a radio transmitter inside the chloroform container sold to the individual. *Id*. at 278. After the individual bought the chloroform, officers followed the signal and traced the individuals to a secluded cabin in Wisconsin. *Id*. They performed intermittent video surveillance on the cabin for three days, after which they obtained a search warrant and discovered the chloroform and the drug laboratory. *Id.* at 278-79.

[116] *Id.* at 277, 279.

diminished expectation of privacy in an automobile because a car that travels on public roads and highways is open to public scrutiny.[117] The defendants did not have a legitimate expectation of privacy regarding information observable to the public such as movements of a car on public property.[118]

The Court also noted that the police did not use a beeper or video surveillance in an intrusive way; rather, it was used as a way to assist the police in obtaining information they could have obtained even *without the use of either technology*.[119] The Court stated that the Fourth Amendment does not prohibit the police "from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[120] The acts of law enforcement were simply enhanced by visual surveillance, and as the Supreme Court stated as early as 1886 in *Boyd v. United States*, "visual surveillance [is] unquestionably lawful because "'the eye cannot . . . be guilty of a trespass.'"[121] The Court in *Knotts* made a distinction between using technology simply to improve the quality and effectiveness of the officials' existing senses as opposed to using the technology to observe evidence incapable of observation using only the senses.

A similar decision was reported in the Ninth Circuit in *United States v. McIver*.[122] This case again involved two different forms of searches conducted by law enforcement. Law enforcement officials placed unmanned surveillance cameras in a remote forest location where they had found marijuana plants being cultivated.[123] After observing the surveillance tapes, the police officers were able to locate the vehicle of one of the individuals on the tape who visited the area.[124] The police officers then performed a second search by placing a tracking device on the undercarriage of the vehicle while it was parked on the defendant's driveway. [125] The defendant argued that the act of placing the

[117] *Id.* at 281 ("'One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects.'" (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974))).

[118] *Id.* at 281-82 (explaining that in traveling on public streets, defendants "voluntarily conveyed to anyone who wanted to look the fact that [they were] traveling over particular roads in a particular direction").

[119] *Id.* at 282 ("Visual surveillance from public places along [the defendants'] route or adjoining . . . premises would have sufficed to reveal all of these facts to the police.").

[120] *Id*.

[121] 116 U.S. 616, 628 (1886).

[122] 186 F.3d 1119 (1999).

[123] *See id*. at 1122. The officer in charge decided to use surveillance cameras as opposed to actually having officers stake out the area due to an insufficient number of officers to maintain a round-the-clock surveillance. *Id.*

[124] *Id.* at 1122-23.

[125] *Id*. at 1123. Although the Court ruled that placing the tracking device on the exterior of the car was not unlawful, Judge Kleinfeld in his concurrence made an important distinction between a "search" and a "seizure," arguing that an unlawful seizure might still take place even in a context where a person's privacy rights have not been infringed. *See id.*

tracking device on the car constituted both a trespass onto the defendant's property and an unreasonable search of the vehicle.[126]

In determining whether this was an unconstitutional search, the Court asked whether the actions of the police officers infringed on an expectation of privacy that society would consider reasonable.[127] The Court explained that since the exterior of a car is out in the public eye and observable by anyone passing by, the owner can hardly expect to keep the surface free from observers.[128] *McIver* clarifies the principle that technology does not offend the Fourth Amendment when it is used in places and situations where people do not have a reasonable expectation of privacy. The use of technology to ease the compilation of information does not make the use unreasonable.[129] The utilization of unmanned cameras was similar to the surveillance in *Knotts*, and, consistent with that decision, the court concluded that the use of video surveillance was just a more cost-effective way of visual observation and was not unconstitutional.[130]

Applying the two-part test to RFID to determine if its use would be considered an unconstitutional search is context-dependent. As the previous cases illustrate, the constitutionality of a search depends on the searched individual's subjective and objective expectation of privacy.[131] Therefore, government use of RFID as a way of tracking the location of vehicles on public roads and highways would likely be allowed.[132] Given the other tracking device cases, a court would likely find that an individual does not

at 1133. He explained that while the placement of the tracking device was in an area where the defendant did not have a reasonable expectation of privacy, it should be treated as a seizure for Fourth Amendment purposes. *See id.* (finding that property is seized when the owner's possessory interest is interfered). Judge Kleinfeld went on to explain that the definition of a seizure is "some meaningful interference with an individual's possessory interests," and that performing mechanical work on the exterior of a person's vehicle infringes on the person's possessory interest in the vehicle. *Id.* (citing United States v. Karo, 468 U.S. 705, 712 (1984)).

[126] *See id.* at 1126.

[127] *See id.* at 1126-27 (citing United States v. Jacobsen, 466 U.S. 109, 122 (1984)).

[128] *See id.* at 1126 (finding that if an object is "thrust" into public view, there is no reasonable expectation of privacy). The McIver Court took this opportunity to highlight the case of *New York v. Class*, 475 U.S. 106 (1986). In that case, a police officer opened the door of the respondent's car to move papers that were blocking from view the vehicles identification number (VIN) located on the dashboard. *Id.* This was held not to violate the Fourth Amendment because the mandated visibility of the VIN "makes it more similar to the exterior of the car than to the trunk or glove compartment." *Id.* at 114.

[129] *McIver*, 186 F.3d at 1125 (finding the use of motion-activated cameras to be a "prudent and efficient use of modern technology").

[130] *Id.* at 1125.

[131] *Id.* (declaring that while McIver may have had a subjective expectation of privacy, such an expectation was not objectively reasonable).

[132] See *id.* at 1127.

have an expectation of privacy regarding the location and the path of a vehicle which is traveling on public property.[133] As in *Knotts*, the use of RFID tags to track vehicles would only enhance law enforcement's natural ability to observe the movement of the vehicle.[134] RFID is more versatile than a simple tracking device. When placed in toll collection booths, the main purpose of the RFID system is to expedite the collection of toll money and reduce traffic.[135] However, this use of an RFID system on the highways provides an additional benefit for the government by compiling information regarding which cars have passed through the tollbooth. Despite the surveillance potential of this RFID system, courts would likely allow a party to admit E-Z Pass records to prove the whereabouts of an individual, because persons traveling on public highways have no expectation to keep the path of their travels private. They are traveling in public space where anyone is free to observe them.

On the other hand, the outcome would be very different if RFID readers situated along highways were able to access personal information about anyone passing along with a RFID chip in his driver's license. Although the driver is traveling through a public place, one could argue that he maintains a reasonable expectation of privacy regarding the information on his driver's license. Unless the driver's license is displayed to the public, he would likely expect that information to remain private. The government, however, could avoid this issue and implement this type of data gathering by informing the public that such a system was in place, thereby destroying any subjective expectation of privacy. This possible circumvention of the public's expectation of privacy has been recognized and addressed by several states.[136] Washington, for example, has adopted privacy laws that provide its citizens with more expansive protection from government intrusion and diminished expectations of privacy.[137]

Another issue brought to light in the foregoing cases is the act of placing a RFID tag on an individual's personal property in order to track him or her, as in the second search conducted in *McIver*.[138] In that case, the Ninth Circuit found that the officer's act of placing a tracking device on the defendant's car, unbeknownst to him, was not unlawful because placement of the device was on

[133] *See, e.g.*, *id*. at 1125; United States v. Knotts 460 U.S. 276, 281-82.

[134] *See Knotts*, 460 U.S. at 282 (indicating that the use of technology to increase sensory capabilities is not a violation of the Fourth Amendment).

[135] Fred Philipson, *Fast Lane*, GOVERNMENT TECHNOLOGY, Sept. 2, 2004, http://www.govtech.net/magazine/story.php?id=91366&issue=9:2004 (describing how RFID technology is making toll collecting more efficient).

[136] *See infra* Section V (describing the efforts of state legislatures and courts to curb the use of new surveillance technologies by the police).

[137] *See* Washington v. Jackson, 76 P.3d 217, 222 (Wash. 2003) (adopting a pro-privacy interpretation of subjective expectation).

[138] United States v. McIver, 186 F.3d 1119, 1126 (1999).

the exterior of the car where there is no reasonable expectation of privacy.[139] Therefore the government, as well as commercial users of RFID, would likely be able to place active RFID tags in various items without the knowledge of the consumer. As long as the consumer does not have a reasonable expectation of privacy where the tag was placed on the item, the implementation would be permissible.

Courts have allowed the use of tracking devices in the cases previously discussed because the tracking devices were seen as enhancing the officers' existing ability to observe.[140] From these cases, it is clear that the use of RFID strictly for tracking and surveillance purposes, similar to beepers and tracking devices, would not be found unconstitutional. However, the RFID implications of these cases are complicated by the fact that RFID can go well beyond just sensory enhancement. RFID surveillance can yield information to the user beyond what would be made apparent by using just a sensory-heightening device. An examination of the use of other more advanced technologies and their interaction with Fourth Amendment law will facilitate a prediction for the future of RFID.

D. *The Pinnacle Case – Thermal Imaging*

Perhaps one of the most instructive cases examining the clash between emerging technology and the potential erosion of privacy rights is *Kyllo v. United States*.[141] Suspecting that the defendant was growing marijuana in his home, police used a thermal imager that allowed them to gain information about the home's interior without any physical entrance onto the property.[142] The scan was performed from a government agent's vehicle parked across the street from the defendant's home and took only a few minutes to reveal that the roof over the garage was relatively hot compared to the rest of the home.[143] After several appeals and remands to the lower courts, the Court of Appeals for the Ninth Circuit allowed the warrant and the search, holding that the use of

[139] *See supra* notes 128-131 and accompanying text (describing the court's rationale for affirming the use of the tracking device).

[140] *See* United States v. Knotts, 460 U.S. 276, 282 (1983) (finding that the Fourth Amendment does not prohibit the police from increasing their sensory capacities through the use of modern technology).

[141] 533 U.S. 29 (2001).

[142] *Id.* at 29. Thermal imaging operates by detecting infrared radiation, which virtually all objects emit but are not visible to the naked eye; the device converts the radiation into images based on relative warmth so in some respects its acts a video camera showing heat images. *Id.* at 29-30.

[143] *Id.* at 30. The agent concluded that the defendant was using halide lights to grow marijuana in his house. Based on this information and tips from informants and examination of utility bills, the government agents subsequently obtained a search of the defendant's home, which resulted in locating more than 100 plants of marijuana. *Id.*

the thermal imager was not unconstitutional.[144] In affirming the district court's decision, the Ninth Circuit "held that petitioner had shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home."[145]

This might prompt the question of whether the defendant felt that he *needed* to conceal the heat. Without knowing that a device such as a thermal imager even existed, the defendant could very well have believed that the heat being emitted from his home was not exposed to the public. This case thus raises the question of whether knowledge of the existence of technology erodes society's expectations of privacy. The lower court's opinion seems to imply that regardless of the defendant's lack of knowledge that the heat could be detected by a thermal imaging device, his privacy rights were not affected.[146] This is the exact point the Supreme Court took up in its decision to grant certiorari.[147]

The Supreme Court first discussed the implications of developing technology and society's expectation of privacy,[148] as well as the effects of such technology on Fourth Amendment privacy rights.[149] The Court emphasized the importance of keeping the right of privacy in the home intact to preserve the purpose of the Fourth Amendment,[150] and stated that the implementation of technology not in "general public use" to obtain information about the interior of a home that could not otherwise have been obtained without physical intrusion constitutes a search under the Fourth Amendment.[151]

The government and the dissent raised several arguments in favor of allowing the technology to be used to obtain information about the interior of the defendant's home. All of these arguments were refuted by the majority, and the analysis developed in the decision is especially applicable to scenarios potentially raised by RFID technology. First, the government argued that use of the device was not a search under the meaning of the Fourth Amendment, because the device only picked up heat radiating from the exterior of the house.[152] The majority quickly refuted this, expressly stating that details of the house's interior that are extracted by advanced technology are still private

[144] *Id.* at 30-31.

[145] *Id.* at 31.

[146] *See id.* (holding that Kyllo had no subjective expectation of privacy, yet ignoring the issue of whether Kyllo knew that the heat could be detected by a thermal imaging device).

[147] *See id*. (discussing the procedural history of the case leading to the grant of certiorari).

[148] *See id.* at 34 ("The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.").

[149] *See id.* at 33-34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

[150] *See id.* at 34.

[151] *Id*.

[152] *See id*. at 35.

information protected by the Fourth Amendment.[153] The fact that the heat was radiating from the interior to the exterior did not convert it into public information.[154] Commenting on the specific technology, the Court stated that "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[155]

RFID technology likely falls within the Court's statement as it is a sophisticated system currently under development. Government officials could use a reader pointed in the direction of a home to determine the existence of particular objects or substances in the home, which have been tagged with an RFID device. This example is very similar to the scenario the Supreme Court predicted in *Kyllo*.[156]

Another argument raised by the government dealt with the nature of the information gathered.[157] The government argued that the use of the thermal imager was not a search because it did not detect private activities or conversations within the home.[158] However, as the majority explained, the "Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."[159] Temperature information about the defendant's home is considered a detail of the home, which should be free from government invasion.[160] The dissent repeatedly stated that the information obtained neither involved the interior of the home, nor revealed "intimate details of the home," and therefore was not unconstitutional.[161] Following this logic, before one could determine if a search is unconstitutional, one would first have to examine the type of information obtained. Making this type of distinction would require "a jurisprudence specifying which home activities are 'intimate' and which are

---

[153] *Id.* at 37 (declaring that Fourth Amendment protection does not depend on the quantity or quality of the information gathered).

[154] *See id*. at 35-36 (indicating that the holding would otherwise severely limit the protection of the Fourth Amendment).

[155] *Id*. at 36.

[156] *See id.*

[157] *See id.* at 37.

[158] *Id.*.

[159] *Id*. The court compares the quantity of information obtained with the manner in which it was obtained:

> In *Silverman* . . . we made clear that any physical invasion of the structure of the home, 'by even a fraction of an inch,' was too much, and there is certainly no exception to the warrant requirement for the officer who barely cracks open the front door and sees nothing but the non-intimate rug on the vestibule floor. In the home . . . *all* details are intimate details, because the entire area is held safe from prying government eyes.

Id. (citing Silverman v. United States, 365 U.S. 505, 512 (1961)).

[160] *See id*. at 38.

[161] *See id.* at 41.

not."[162] For example, many people may consider the information contained in a passport to be personal information over which they have an expectation of privacy. However, the number of passports in a house may seem like a non-intimate piece of information. If such a jurisprudence was actually developed, it would be impractical to apply because "no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up 'intimate' details –and thus would be unable to know in advance whether it is constitutional."[163]

Accordingly, any kind of information regarding the interior of a home and gathered with RFID technology would likely be found to be the product of an unconstitutional search. Further, parsing the definition of "intimate" information is unnecessary. Regardless of the perception of the quality or quantity of information, any data gathered from a constitutionally protected place, such as a home, would likely not be admissible.

One of the main concerns in *Kyllo* arises from the assertion that the technology used by the government was not in "public use."[164] This prompts the question of what the outcome would have been had thermal imaging been a more widely-known. Will the Fourth Amendment no longer protect individuals from this same privacy invasion fifty years from now when the technology is in "public use"? It is conceivable that under the Court's reasoning in Kyllo, RFID technology could become so widespread that an expectation of privacy no longer exists in even an individual's home. The existence of tags in all consumer items, passports, driver's licenses, smartcards, etc., and the existence of RFID readers could eventually become common knowledge and erode society's expectation of privacy. Will the government, private companies, and anyone who can obtain a reader be free to collect as much information as they please? Some states have addressed the slippery slope of privacy erosion through evolution and awareness of new technology.[165]

IV. THE BALANCE BETWEEN GOVERNMENT ACTION AND ACTS BY A PRIVATE PARTY

Fourth Amendment cases interpreting the scope and definition of a search have been limited to actions by government officials, not those undertaken by public officials in conjunction with private parties. The question remains as to the limits of the government's power when it acts in concert with or subsequent to invasive actions by private parties. Defining constitutionally-acceptable behavior when government officials conduct a search to which a

[162] *Id*. at 38-39.

[163] *Id*. at 39.

[164] *See id.* at 34 (indicating that the uncommon nature of the thermal imaging device makes it more likely to constitute an unlawful search).

[165] *See infra* Part V (highlighting the growth of state regulations on surveillance technology).

private party has also contributed is of paramount importance to the issues raised by RFID technology. Due to the large number of private organizations that will soon be using RFID to gather information about consumers, there is a legitimate need to define the government's right and ability to obtain and use such information, especially if a private party has obtained information by invading an individual's privacy.

While *Katz* and *Silverman* broadened the definition of a search and increased the protection offered by the Fourth Amendment, the Amendment's reach was limited by the Supreme Court decision of *United States v. Jacobsen*.[166] The *Jacobsen* Court explained that although the Fourth Amendment's definition of "search and seizure" reaches government conduct, it does not reach a search, even if unreasonable, conducted by a private party.[167] The *Jacobsen* Court found the Fourth Amendment wholly inapplicable "to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official."[168]

Jacobsen provided a unique perspective to Fourth Amendment law due to the circumstances of the case; namely, the intervening actions of a private party, the carrier of a package, and the subsequent seizure of the substance in the package by government officials.[169] Due to the private character of the intervening party, the Court ruled that the party's actions were not subject to Fourth Amendment scrutiny, regardless of whether its actions were accidental or deliberate, reasonable, or unreasonable.[170] *Jacobsen*, therefore, holds that only the government's actions, subsequent to the private party's invasion of the defendant's privacy, are examined and tested under the Fourth Amendment.[171] Further, when private information is first revealed to a third party such as the private carrier in *Jacobsen*, the government's subsequent use of the

[166] 466 U.S. 109 (1984).

[167] *See id.* at 113 (stressing that the Court's Fourth Amendment precedent differentiates between private and governmental action). This principle was first announced in the case of *Walter v. United States*, 447 U.S. 649, 656 (1980). In that case, a private party opened a misplaced package and found motion picture films that appeared to be contraband. *Id.* at 651-652. The private party turned the films over to FBI agents, who proceeded to view the contents without first obtaining a search warrant. *Id.* at 652. The Supreme Court held the search to be unconstitutional. *Id.* at 659. The Court ruled that while government officials may reap the benefits of an invasive search by a private party, the Government does not have the right to exceed the scope of the private search. *Id.* at 657.

[168] *Jacobsen*, 466 U.S. at 113 (quoting *Walter*, 447 U.S. at 662).

[169] *See id.* at 111-12. *Jacobsen* involved a package containing cocaine that was being sent to the defendant and which was damaged in transmit. The carrier of the package, noticing a white powdery substance coming from the package, opened the package, and called federal agents who took a sample of the substance without a warrant. *Id.*

[170] *See id*. at 115.

[171] *See id*.

information is not a violation of the Fourth Amendment.[172] The Court stated, "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information."[173] In *United State v. Miller*, the Supreme Court further stated that

> the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[174]

Although *Jacobsen* and *Miller* seem to have given the government latitude when conducting searches after a private party has intervened, an earlier case set some boundaries that the government is not permitted to cross. One of the first cases dealing with an intervening third party is *Walter v. United States*.[175] In *Walter*, a private party opened a misdirected package and discovered motion picture films that appeared to be contraband.[176] The private party turned the films over to the FBI, which viewed the contents without first obtaining a search warrant.[177] The Supreme Court ruled the search unconstitutional.[178] The Court held that although government officials can reap the benefits of an invasive search by a private party, the government does not have the right to *exceed the scope of the private search*.[179]

The Supreme Court's caselaw clarifies the extent to which the government can benefit from the findings of a search conducted by a private party using intrusive technology. Certain principles relevant to RFID technology emerge from that caselaw. First, the Fourth Amendment only protects against an unreasonable search and seizure performed by the government and does not reach the actions of private parties. Therefore, information gathered initially by a third party is not protected by the Fourth Amendment because its purpose is to protect against government action. Second, the government is not prohibited from using information obtained by a private party, regardless of the manner in which it was obtained. Finally, while the rules may increase government's access to information it otherwise could only not access without

---

[172] *See id*. at 115.

[173] *Id*. at 117.

[174] United States v. Miller, 425 U.S. 435, 443 (1976) (finding that a depositor takes a risk that personal information might be given to the government).

[175] *See* Walter v. United States, 447 U.S. 649, 651-52.

[176] *Id*. at 651.

[177] *Id*. at 652.

[178] *Id*. at 659.

[179] *See id*. at 657 ("If a properly authorized official search is limited by the particular terms of its authorization, at least the same kind of strict limitation must be applied to any official use of a private party's invasion of another person's privacy.").

a search warrant, any subsequent search conducted by the government beyond the private parties' actions, is subject to Fourth Amendment scrutiny.

These principles allow the government access to a great deal of information that private companies may have gathered using RFID systems. As discussed previously, widespread commercial use of the technology is developing quickly.[180] As more companies and organizations begin using RFID, massive amounts of consumer information will be accumulated. This information, gathered by private parties and not the government, is not subject to Fourth Amendment scrutiny. However, after the information is gathered by a private party, few barriers exist to prevent the government from compiling and gathering all that information. As *Jacobsen* explained, use of the information by the government is not unlawful unless government officials have performed subsequent actions that expand on the search in an unlawful way. Whether the *private organization* gathered the information in a lawful way or not does not affect the constitutionality of the government's use of it. As mentioned earlier, the government is able to contract with private parties and has already begun to do so to obtain information gathered through private parties' use of RFID.[181] The Fourth Amendment will not be implicated in analyzing the actions of the private parties, but the government is subject to Fourth Amendment scrutiny for any actions that may further the research and data gathered by the private party.

V. STATES' RESPONSES – A MORE STRINGENT APPROACH

Although the previously- discussed cases involving surveillance technology exhibit a trend of allowing government officials a high degree of leniency to use new surveillance technologies, several states have attempted to protect their citizens from this potentially slippery slope. Some states have taken actions to ensure their citizens protections beyond the Fourth Amendment. At least one state has concluded that, as with beepers, the installation of tracking devices even on the exterior of a vehicle constitutes an impermissible search under the State's constitution and have held fruits of such seizures inadmissible.[182] Another state, through its state constitution, offers broader protection against invasions of privacy than does the Fourth Amendment of the

[180] *See supra* text accompanying notes 18-21.

[181] *See supra* Part II (explaining how commercial uses of RFID are being used in criminal investigation).

[182] *See* Saldana v. Wyoming, 846 P.2d 604, 658 (Colo. 1993) (citing several cases in which the State courts interpret the State Constitution to provide more protection than the Fourth Amendment, including People v. Oates, 698 P.2d 811 (Colo. 1985) (holding that warrantless installation of an electronic tracking device in a drum of chemicals prior to sale violated the purchaser's right to protection from unreasonable searches under the Colorado Constitution), and People v. Sporleder, 666 P.2d 135 (Colo. 1983) (holding that warrantless installation of a pen register to record numbers dialed from defendant's home telephone constituted an unreasonable search under the Colorado Constitution)).

United States Constitution.[183] An examination of these state protections sheds some light on the likely future reception of RFID technology in the courts.

Washington State's constitution adopts a broad view of what constitutes an invasion of privacy; the right to privacy under the constitution is "not confined to the subjective privacy expectations of modern citizens who due to well publicized advances in surveillance technology are learning to expect diminishing privacy in many aspects of their lives."[184] *Washington v. Jackson* looks closely at the effects of technology on society's expectation of privacy.[185] Unlike previous Supreme Court decisions, the *Jackson* court made a distinction between tracking devices such as Global Positioning System (GPS) technology and mere sense-enhancing equipment such as flashlights and binoculars.[186] GPS technology consists of a network of satellites and receiving devices that are used to accurately compute the position of items around the globe.[187] While GPS technology provides many comforts and conveniences to consumers, it also provides advantages and information-gathering opportunities to law enforcement officials.[188] In recognizing that the use of sense-enhancing technology such as binoculars or a flashlight does not violate the Fourth Amendment, the Supreme Court of Washington quoted an earlier case, stating that a "particularly intrusive method of viewing[] may constitute a search."[189]

---

[183] The Washington Constitution states that "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law." WASH. CONST. art. I, § 7. The state constitution has been interpreted to be "more protective than the Fourth Amendment." Washington v. Jackson, 76 P.3d 217, 222 (Wash. 2003); *see infra* note 182.

[184] Washington v. Young, 867 P.2d 593, 597 (Wash. 1994) (citing Washington v. Myrick, 688 P.2d 151, 154 (Wash. 1984)).

[185] *See Jackson*, 76 P.3d at 222.

[186] *See id.* at 222-23 (arguing that devices that only make more readily observable what is already public are constitutional, while tracking devices may, in certain circumstances, be unlawful).

[187] *See* Wikipedia: GPS, http://en.wikipedia.org/wiki/Gps (last visited Jan. 25, 2006).

[188] *See, e.g.*, Press Release, California Department of Corrections and Rehabilitation, California Department of Corrections and Rehabilitation Announces GPS Partnership with the City of San Bernardino to Monitor High-Risk Gang Activity (Mar. 14, 2006) at http://www.corr.ca.gov/Communications/press20060314.html; Jim McKay, *Nowhere to Hide*, GOVERNMENT TECHNOLOGY, June 2004, http://www.govtech.net/magazine/sup_story.php?id=90490&magid=17&issue=6:2004.

[189] *Jackson*, 76 P.3d at 222 (citing *Young*, 867 P.2d at 598) (emphasis omitted). The court also drew a comparison between GPS technology and the use of thermal imaging by government officials. *See id.* (declaring that the use of such thermal imaging is intrusive under the Washington constitution). Thermal imaging is a method by which police officials are able to detect the presence of drugs inside a structure by pointing a device at the structure from the outside at a distance. *See, e.g.*, Kyllo v. United States, 533 U.S. 29, 30 (2001). The detection of the drugs is possible because heat is generated by grow lamps used for drug cultivation. *Id.*

The Supreme Court of Washington overruled the court of appeals, which had held that the use of GPS devices was equivalent to merely following the defendant on public roads where he voluntarily exposed himself to public view.[190] In comparing GPS with sense augmenting devices, the Supreme Court of Washington stated that "unlike binoculars or a flashlight, the GPS device does not merely augment the officers' senses but rather provides a technological substitute for traditional visual tracking."[191] The court continued by explaining how an officer, using only his unaided vision, would likely be incapable of performing the type of tracking a GPS device provides.[192]

In addition to finding that GPS facilitated a superhuman degree of visual tracking, the court also considered the particular type of information the GPS technology provided.[193] The court observed that the GPS device allowed its users to obtain a great deal of information about an individual's life.[194] Some examples of the types of information discussed include a "detailed record of travel to doctors' offices, banks, gambling casinos, . . . place of worship, political party meetings, . . . places where children are dropped off for school, . . . the family planning clinic, the labor rally."[195] In other words, the places that people visit can "provide a detailed picture of one's life."[196] The Court ultimately concluded that a warrant was required before a tracking device such as a GPS locater could be attached to a vehicle, even if the device was only tracking movement in public places.[197] The Court stated that the citizens of Washington "have a right to be free from the type of governmental intrusion that occurs when a GPS device is attached to a citizen's vehicle, *regardless of reduced privacy expectations due to advances in technology*."[198] Without the protections afforded by the state laws and State of Washington Constitution, the defendant would have likely been left unprotected, as the Fourth Amendment offers only scarce protection to individuals in public areas.[199]

---

[190] *See Jackson*, 76 P.3d at 223 (finding that, unlike binoculars, GPS devices do not merely augment an officer's senses).

[191] *Id*.

[192] *See id.* The court commented that "[i]t is unlikely that the sheriff's department could have successfully maintained uninterrupted 24-hour surveillance [over two and a half weeks] by following [the defendant]." *Id.* The court concluded that there was a "difference between the kind of uninterrupted, 24-hour a day surveillance possible through use of a GPS device, which does not depend upon whether an officer could in fact have maintained visual contact over the tracking period, and an officer's use of binoculars or a flashlight to augment his or her sense." *Id.*

[193] *Id.*

[194] *See id.*

[195] *Id.*

[196] *Id*.

[197] *See id*. at 224.

[198] *Id*. (emphasis added).

[199] *See* United States v. Knotts, 460 U.S. 276 (1983); Karim, *supra* note 31, at 502-03.

In deciding *Jackson*, the Washington court looked to another state which also has found federal Fourth Amendment protection inadequate to protect citizens against the government's increasingly intrusive technologically-enhanced searches. Oregon addressed the issue in *State v. Campbell*.[200] In that case, police officials, after unsuccessful visual tracking, attached a radio transmitter to the defendant's vehicle in order to track the movements of a suspected burglar.[201] The *Campbell* decision hinged on whether the "use of a radio transmitter to locate a private automobile to which the transmitter has been surreptitiously attached is a 'search' or 'seizure' under . . . the Oregon Constitution."[202] The court determined that the search was unconstitutional because "the police did not have a warrant to use the transmitter, and because no exigency obviated the need to obtain a warrant."[203] In reaching its decision, the court compared the Oregon Constitution's privacy protections with the Fourth Amendment test for determining an invasion of a reasonable expectation of privacy.[204] The court found that the Fourth Amendment reasonable expectation of privacy determination largely depends on whether the "search," and more specifically the radio transmitter, was in a private place or a public place.[205] The court expressly rejected the "reasonable expectation of privacy" test to define the parameters of the privacy provisions of the Oregon state constitution.[206] The court stated that the privacy protected by its Constitution is "not the privacy that one reasonably *expects* but the privacy to which one has a *right*."[207]

---

[200] Oregon v. Campbell, 759 P.2d 1040, 1049 (Or. 1988).

[201] *See id.* at 1041-42. This case demonstrates that GPS and tracking devices are more than just a mere sense-enhancing technology, and that they allow police enforcement to conduct surveillances that were not possible prior to the use of such devices. *See id.* at 1045. Police officials suspected the defendant of burglaries and made several unsuccessful attempts to follow his automobile. *See id.* at 1041. "The rural area made it difficult to follow defendant closely without detection, and defendant began to drive evasively after becoming aware of the efforts to follow him. Having failed to follow defendant visually, [the police] decided to follow him by means of a radio transmitter attached to his automobile" *Id.*

[202] *Id.* at 1041.

[203] *Id.* at 1049.

[204] *See id.* at 1043-44.

[205] *See id.* at 1044.

[206] *See id*. (stating that the test masks the "various substantive considerations" of Fourth Amendment searches). The Oregon Constitution provides:

> No law shall violate the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search, or seizure; and no warrant shall issue but upon probable cause, supported by oath, or affirmation, and particularly describing the place to be searched, and the person or thing to be seized.

OR. CONST. art. I, § 9.

[207] *Id*. at 1044 (emphasis in original).

The court also made a distinction between a radio transmitter and a sense-enhancing device, stating that a "transmitter has nothing to do with vision; it broadcasts a signal that enables the police to locate . . . the transmitter from anywhere that its signal can be received."[208] The court rejected the State's argument that the search was not conducted on a "protected premises."[209] Instead, the court held that the decision needs to be made based on the actions taken by the police official, and not necessarily on where the actions took place, stating that "[u]sing a transmitter is either a search or it is not . . . [and] cannot depend upon the fortuity of where the transmitter happens to be taken by the person under observation."[210] This statement exemplifies the difference in the interpretation of privacy rights between the Oregon Supreme Court under the Oregon Constitution and the United State Supreme Court under the Fourth Amendment. State courts have become increasingly aware of the inadequacies of the Fourth Amendment's protection in the face of emerging technology and the way in which they can work to significantly reduce society's legitimate expectation of privacy.

This type of broad protection against the use of surveillance technology could also have an effect on RFID use. Unlike the Ninth Circuit in *McIver*,[211] the Supreme Court of Washington found that the use of electronic surveillance allowed law enforcement officials to perform searches beyond those that could be performed by unaided human abilities.[212] Similarly, RFID tracking along highways or in remote locations could be found to be beyond the normal sensory abilities of officers and held unconstitutional under state laws. This type of distinction would have to be scrutinized on a case-by-case basis. The Washington and Oregon cases discussed, however, demonstrate the possibility that enhanced surveillance, even performed in public places, may violate privacy rights.

In *Washington v. Jackson*, the Supreme Court of Washington also commented on the specific content of information gathered, finding that it revealed private details of the individual's life.[213] RFID has a considerably greater capacity and ability to communicate information than a GPS device. In light of these observations, much of the information gathered by RFID, such as

[208] *Id*. at 1045.

[209] *See id*. at 1046. The State first argued that the transmitter only disclosed information that was readily available to the public eye and was therefore a sense-enhancing device that didn't violate the privacy rights of the defendant. *See id.* at 1044-45. The State also contended that the defendant didn't have a privacy right where the observations were made and there would only have been a violation of the defendant's privacy rights if the police had conducted a search in a protected area such as the defendant's home. *See id.* at 1046.

[210] *Id*. at 1047.

[211] *See supra* notes 128-130 and accompanying text.

[212] *See supra* note 186 and accompanying text.

[213] Washington v. Jackson, 76 P.3d 217, 223 (Wash. 2003) (finding that the device could reveal information about "preferences, alignments, associations, personal ails, or foibles").

tracking a person's local routine or information regarding where they have traveled (extracted from a passport), could be seen as protected information that should not be obtained without a warrant. Aside from passports, RFID tags in consumer products could reveal an individual's lifestyle, habits, and preferences. The question of whether the details revealed by the RFID data compilation is intimate information subject to privacy protections must be resolved by the courts.

CONCLUSION

Previous cases involving the use of technology to perform searches and gather information demonstrate that the lawfulness of the gathering party's actions depends on many factors. Litigation regarding information gathered through use of RFID is likely to depend on similar factors, and decisions are likely to be found on both sides of the line. These factors include whether RFID impinges on a subjective and objective expectation of privacy regarding the information obtained through use of the technology. Used as a simple tracking device, RFID searches are likely to be constitutional, because tracking devices in public places are not considered to violate an objective expectation of privacy. However, when gathering sensitive information about an individual or from locations private to the individual, such as their homes, the individual's expectation of privacy affects the determination of lawfulness under the Fourth Amendment. Whether the specific information gathered is "intimate" or not is also a factor in the decision.

The biggest long-term concern for individuals may be retaining their subjective expectation of privacy in the face of emerging surveillance technology. As society becomes more accustomed to technology and its ability to gather information, society will likely lose some of its expectations of privacy in actions that involve that technology. If the use of RFID readers in airports becomes so widespread that when an individual walks into an airport, he expects the information on his passport to be available to government officials in the airport, then gathering that information could likely not be seen as a violation of the Fourth Amendment. While this may sound like an alarming proposition, many states are taking actions to protect its citizens from completely losing all expectation of privacy.